EXECUTIVE SUMMARY

Delivering innovative IP-based services and applications to enterprises requires a robust and secure MPLS-enabled virtual private network (VPN) or IP-based VPN. Emerging virtual private cloud (VPC)-based services also rely on the underlying network, which is the environment in which any cloud service must exist. The secure connectivity of a private IP VPN service combined with the data security supplied from a VPC service ensures that a customer's data and applications have the high availability, reliability, and flexibility to connect to any enterprise resources.

This IDC White Paper discusses the following:

- The MPLS VPN offers enterprises a unique opportunity to operate existing high-speed data, voice, and video enterprise applications over the VPN with inherent security, quality of service (QoS), and low latency and combine these features with new virtualized, cloud services for on-demand access.
- Enterprises are more likely to select managed network services such as managed security, hosted VoIP, and managed storage from a communication service provider (CSP). These CSPs can integrate a network VPN service with support for new VPC services such as datacenter connectivity and SaaS that have the same QoS levels and SLAs.
- AT&T's IP-enabled network extends the use of the AT&T MPLS-enabled VPN to adapt, understand, control, and optimize IP data applications between enterprise offices and public and private datacenters.
- Enterprises prefer to choose an MPLS-enabled network that automatically adapts to new applications, including future virtualized or cloud service schemes that enable WAN communication between datacenters, compute resources, and storage resources and that can guarantee the performance and QoS of each cloud computing flow.
IN THIS WHITE PAPER

This IDC White Paper examines the market opportunity for next-generation IP business services that are enabled by an MPLS/IP VPN and how enterprise applications can benefit from advanced MPLS VPN solutions.

MARKET OVERVIEW AND ENTERPRISE TRENDS

Market Overview

Today's enterprise managers have fewer IT resources, yet they still have to make the necessary investments to keep pace with the requirement of supporting new applications and higher amounts of data bandwidth. More often, the IP VPN is the most important component of a managed network service, as enterprises increasingly depend on VPNs to support VoIP, enterprise data, storage, and security applications.

In addition to maximizing performance while minimizing costs, IP VPNs offer the ability to prioritize delay-sensitive applications such as VoIP by class of service (CoS), create and improve disaster recovery infrastructures, utilize a fully meshed infrastructure that replaces outdated hub-and-spoke architecture, and reduce complexity to simplify network management in an increasingly complex landscape.

The next decade will see enterprises employ a wide range of commercial software, cloud, and mobile IP-based applications, which raises the importance of robust WAN IP connectivity solutions that will include the use of more on-demand network resources. Enterprises are evaluating and adopting hosted or cloud WAN solutions for selected applications such as VoIP, UC, storage, or video. The cloud WAN solution can be either private (on-premise) or public (hosted offsite). Normally, hosted services imply that a fixed set of computer resources are made available. The economic appeal of cloud (elasticity, pay for what you use, self-service) resonates with both in-house and third-party hosting enterprises.

CSPs with advanced MPLS/IP networks that enable a flexible IP VPN service will be well positioned to deliver a broad and compelling range of enterprise-class IP-based services, including VPC-based services. At the same time, service providers will have to simplify the enterprise end-user experience with easy-to-use, self-service Web portals that are intuitive.

In the business segment, midsize and large enterprises' increasing use of IP VPN and Ethernet WAN communication services comes with expectations that these services will be capable of supporting increased data capacities, real-time data transactions, VoIP, and videoconferencing. This complexity is also driving increased enterprise interest in managed VPN services, application awareness, and use of CoS, according to IDC's 2014 U.S. Enterprise Communications Manager Survey. VoIP penetration grows stronger, with 55% of respondents using MPLS IP VPNs to transport VoIP traffic over their networks in 2014, compared with 52% in 2012 (see Figure 1). Another indicator is that IP applications are driving more managed CPE usage, which increased from 34% in 2012 to 37% in 2014, with increasing use of data/voice/video over VPNs.
FIGURE 1

Enterprise IP VPN Usage Trends

Q. What features do you currently use on your network-based MPLS IP VPN? Select all that apply.

Base = respondents who use network-based MPLS IP VPN

Source: IDC's 2012 U.S. WAN Manager Survey and 2014 U.S. Enterprise Communications Manager Survey

Enterprise Trends and Opportunities: Business VPN and Cloud Services

Overview

While enterprise managers have fewer resources today, they still have to make the necessary investments. Often, the IP VPN is the most important component of the managed network service, as enterprises increasingly depend on VPNs to support VoIP, enterprise data, storage, and security applications.
At the same time, enterprises are evaluating and adopting either public cloud services, which are shared among unrelated enterprises and consumers using the Internet, or private cloud services, which are shared within a single or group of enterprises — with restrictions on access for selected applications such as VoIP, UC, storage, or video. The private cloud solution can be a dedicated or VPC service managed by a CSP. The dedicated private cloud service is similar to a typical hosted CSP solution and implies that there is a fixed rate to pay by month or by number of servers and network resources dedicated for a specified enterprise. The VPC service benefits both CSPs and enterprises because physical compute and network resources are shared and not dedicated to a single enterprise, and the CSP has the flexibility to scale infrastructure on an as-needed basis with tiered options for secure access.

**Market Opportunities**

IP VPNs continue to represent the largest segment of managed network services, accounting for over 55% of the estimated $71.9 billion worldwide managed network services market in 2013. Also, according to IDC’s 2014 *U.S. Enterprise Communications Manager Survey*, more than 50% of enterprises manage all or part of their own DIY VPN with internal IT resources, with this trend toward managed VPN. IDC forecasts that global demand for network-based IP VPN services will grow to $55 billion by 2018.

IDC estimates that the U.S. hosting infrastructure services market, which includes VPC services, will expand from $14.2 billion in 2014 to $18.3 billion in 2018 and that the private cloud service delivery portion of the market will grow from approximately $3.5 billion in 2013 to nearly $10 billion in 2018. Most CSPs are evolving toward support for application-based services and are attempting to position themselves in various parts of the cloud services landscape. IDC research indicates that more than 30% of enterprises are willing to pay a CSP a premium for a managed private cloud service that supports any combination of hosted VoIP, Web, storage, or SaaS leveraging the inherent QoS of an MPLS/IP VPN service to host these cloud services.

Three factors will combine to transform the private cloud services market and the competitive landscape during the next several years:

- Industry consolidation
- The emergence of pure-play "native cloud" infrastructure-as-a-service (IaaS) providers
- Existing CSP hosting providers’ efforts to transition to cloud delivery service offerings

**ENTERPRISE CRITERIA FOR ADOPTING IP APPLICATIONS OVER MPLS VPNs**

Enterprises’ expectations for service quality for their IP VPNs are becoming increasingly important as some of these applications, such as VoIP, are delay sensitive and require lower latency. At the same time, enterprises have also been reticent to embrace mission-critical VPC applications delivered over the Internet because of the lack of:

- Performance
- Security
Enterprises are seeking consistent application performance from the current IP VPN service and any potential VPC service provider, and enterprises are increasingly expecting their CSP to have the necessary IT and application expertise to manage the combination of MPLS VPN services and private cloud services from the same network. Enterprises expect network management tools and a unique customer portal.

Figure 2 illustrates how a CSP can offer the benefits of using the corporate MPLS VPN service to interconnect enterprise sites and applications with the flexibility of supporting VPC services, such as managed datacenters with inherent security, QoS, and latency requirements, versus an Internet-based cloud solution.

**FIGURE 2**

Virtual Private Cloud: Optimized for the Enterprise

- **Public Cloud Operator**
  - Provisioned and Managed IPSEC tunnel
  - No CoS for Enterprise Cloud apps
  - Susceptible to DDoS

- **AT&T**
  - Reduction in Data Center Bandwidth
  - CoS for Cloud application complements existing MPLS VPN CoS
  - Isolation from Internet and DDoS

Source: AT&T, 2015
Enterprise Applications

The ability to prioritize applications by CoS has been a key driver for many enterprises in adopting IP VPNs. To execute CoS, an enterprise must identify its most business-critical or delay-sensitive applications and then assign priorities through CoS settings. Service providers frequently offer three to six classes of service, with naming conventions that vary depending upon the provider. The CoS setting assigned to an application dictates its priority in traveling the network. For each class of service, the service provider specifies a bandwidth threshold, or maximum, depending on total circuit size, number of classes, and contract agreement.

In one enterprise, for example, VoIP and Oracle might be the most business-critical applications set for the highest priority, with email and Web browsing receiving lower assignments. The customer configures its router to tag the correct class in the IP header — DiffServ or TOS bit settings — and pass the data to the service provider's edge router.

If this enterprise then decides to implement SAP in the next six months, it is important to consider what the impact will be of the new high-priority application on the existing high-priority applications. Networks and applications are continuously evolving, and CoS settings will need to be tuned to ensure the continued performance of applications.

For example, if the same enterprise also introduces salesforce.com as an additional new high-priority application, how can the enterprise ensure that the other apps are not affected? In IDC's opinion, the enterprise can expect better performance utilizing a CSP's MPLS VPN service with VPC compared with using a public Internet-based cloud service to support salesforce.com.

Assigning a high-priority CoS to salesforce.com can produce a domino effect in the network and impact the SAP, Oracle, and VoIP applications. What is even more challenging is when the enterprise introduces another new, custom financial application, which may push the highest-priority class to exceed the threshold, causing one or more of the other applications in the same class to drop one class lower, and so on.

Application performance management tools can ensure that all of these IP applications are enabled to maintain consistent performance and QoS. Such tools can be used to monitor utilization for each individual CoS and measure whether usage is above or below threshold allocations. Exceeding a threshold allocation requires the enterprise to either upgrade its circuit for additional bandwidth or move one or more applications to another CoS.
VPN REQUIREMENTS TO SUPPORT ADVANCED APPLICATIONS

Service providers can bring additional value to the enterprise by offering VPC services as a managed service delivered from a network-based MPLS VPN, ensuring service performance, service quality, and managed security from the customer premise to the hosted cloud datacenter.

Offering VPC services is a logical extension to the managed services currently being offered by CSPs because VPC services leverage the QoS, VPN, and private MPLS/IP network assets of the CSP.

The AT&T VPN solution supports service differentiation between a VPC offering from public or Internet cloud providers by employing a direct path from a remote site to a VPC service over the MPLS VPN, reducing network latency and guaranteeing performance. Employing CoS for cloud applications that complements existing IP VPN CoS ensures service delivery for latency-sensitive cloud applications. CSPs can also ensure the higher 99.99% network availability and SLAs that enterprises are accustomed to for VPC-based services, compared with IPSec-based public cloud providers that cannot guarantee equivalent SLAs (refer back to Figure 2).

A CSP can also reduce the bandwidth required to connect enterprise datacenters by using the same VPN connections, compared with a public cloud operator that has to provision extra datacenter circuits to connect to both the VPN and the public cloud network. There is no requirement for a separate managed CPE router to support IPSec, which is the case for public cloud services that are also susceptible to DDoS attacks (refer back to Figure 2). Network elasticity and cloud elasticity work in tandem, and capacity and network profiles can easily be changed for growing capacity needs without forklift provisioning and reconfiguration.

The AT&T VPN offers application management solutions supported over virtualized infrastructures and delivered over a VPN supporting Oracle, SAP, IBM, and Microsoft applications.

One of AT&T’s private cloud service offerings, Synaptic Compute as a Service (CaaS), enables enterprises to use their MPLS VPNs to dynamically connect to an infrastructure service, so AT&T turns up the virtual machines for the customer with CoS. If the customer has a mobile service from AT&T, CaaS enables mobile devices to securely connect to the AT&T VPN, as shown in Figure 3.

Enterprise customers mark traffic leaving their virtual machines with a CoS. Those markings will be honored when the traffic hits the MPLS VPN. Most importantly, the markings will be honored when the traffic leaves the VPN and heads to enterprise branch sites where the cloud traffic is mixed with other traffic on the VPN.
With increased video on demand (VOD), wireless, WiFi, and other BYOD devices such as (smartphones, tablets) accessing the enterprise IP VPN, CSPs need to leverage the IP VPN to support and optimize the quality of experience to the end user. Managing traffic flows to improve IP-enabled applications and support for more real-time collaboration applications from remote, branch, and home office locations is becoming a de facto requirement.

As service providers add cloud services to business VPNs, they are leveraging technologies to create operational simplicity. Business cloud or private cloud services can become a significant network management challenge to SPs as they manage the virtualization of shared router infrastructure. SPs that have the flexibility of bundling a suite of managed business cloud services for business customers over their existing MPLS/IP VPN connections have a competitive advantage.
Monetizing Enterprise VPN and Cloud Services

The market opportunity for CSPs that have the right expertise and the right type of network routing solution is real, and according to results from IDC’s 2014 U.S. Enterprise Communications Manager Survey, over 46% of enterprise respondents are already migrating their workloads from a hosted environment to a cloud provider. Most importantly, they are also switching to a new service provider.

A key challenge for SPs is monetizing the combined managed VPN plus cloud service offering. A typical VPN solution includes port charges, access charges, and CoS charges per port. This model is different from those of some VPC-based service offerings, such as Web hosting or storage, which are billed on a customer basis. IDC believes that SPs that already offer a VPN service should become creative in charging for private cloud services and amortize these services on a per-port basis.

FUTURE OF IP APPLICATIONS OVER VPNs

Moving more mission-critical enterprise software applications into the cloud will place greater emphasis on delivering QoS, reliability, and security. Widespread adoption of SaaS solutions will largely depend on delivering quality of service, reliability, and security. These attributes will be critical for private cloud service providers to ensure a high level of customer service and satisfaction.

While IDC believes the SMB opportunity for both IP VPNs and private hosted cloud services is significant for SPs, this segment has not been penetrated in a broad manner. In the future, SPs that employ more automation tools and automatic application-aware features that adapt to dynamic enterprise application requirements will benefit as enterprises look to take advantage of on-demand features of the IP VPN.

Future advances in managing application sessions and access will also play a key role in enabling IP applications from 3G/4G, broadband, and WiFi hotspots and enable enterprises to prioritize between "lowest cost per bit" and lowest latency by offering a choice of VPN access technologies including Ethernet, private line, broadband, cellular, and WiFi.

Enterprises expect more network management data and simpler tools to increase visibility into actual network application performance via a customer portal. CSPs that have the flexibility of bundling a suite of managed business cloud services for business customers over their existing managed MPLS/IP VPN connections will have a competitive advantage.

IDC predicts that service providers that add VPC service offerings to business IP VPNs will be able to better leverage the technologies and network assets to create operational simplicity and improve their customer "stickiness" for managed IP VPN services and future private cloud-based services.
About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2015 IDC. Reproduction without written permission is completely forbidden.